



Encentuate[®] AccessAssistant and Web Workplace

Deployment Guide

Product version 3.5

Document version 3.5 (Release Candidate)

Copyright notice

Encentuate[®] AccessAssistant and Web Workplace version 3.5

Copyright © August 2007 Encentuate[®]. All rights reserved.

The system described in this guide is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Any documentation that is made available by Encentuate is the copyrighted work of Encentuate and is owned by Encentuate.

NO WARRANTY: Any documentation made available to you is as is, and Encentuate makes not warranty of its accuracy or use. Any use of the documentation or the information contained herein is at the risk of the user.

Documentation may include technical or other inaccuracies or typographical errors. Encentuate reserves the right to make changes without prior notice.

No part of this document may be copied without the prior written approval of Encentuate.

Trademarks

Encentuate[®] is a registered trademark in United States of America, Singapore and United Kingdom. Transparent Crypto-Identity, IAM, Encentuate AccessAgent, Encentuate AccessStudio, Encentuate USB Key and Encentuate Wallet are trademarks of Encentuate[®]. All other trademarks are the property of their respective owners.

Contact information

For more information about this product or any support enquiries, contact us:

To log a support incident: <http://support.encentuate.com/customerservice/>

To reach us by phone:

- Singapore/Asia Pacific: +65-6471-1855
- USA: 1-800-ENCENTUATE

Table of Contents

Copyright notice	ii
Trademarks	ii
Contact information	ii
Conventions and Terminologies	1
Solution Overview	5
Product Specification	5
Web Automatic Sign-on	5
Reverse Proxy	6
User Sign-up	6
Self-service	6
Optional Two-factor Authentication	7
Synchronization of Wallets, AccessProfiles and Policies	8
Centralized Audit Logging	8
Integrated with SSL VPN	8
Deployment Options	8
AccessAssistant	9
Web Workplace	9
Summary of AccessAssistant and Web Workplace Features	13
General Prerequisites	14
Use of Supported Web Browsers	14
Cookies and JavaScript Enabled	14
Installing AccessAssistant or Web Workplace	15
AccessAssistant and Web Workplace Configuration	16
Upgrading AccessAssistant and Web Workplace	16
Embedding Web Workplace in Enterprise Portal	17
Managing Policies	17
User Policy Settings (Through AccessAdmin)	17
System Policy Settings (Through AccessAdmin)	18
Setting automatic web sign-on for AccessProfiles	19
Using the Web AccessProfile Wizard	20
Workflow and Use Cases	22
Web Automatic Sign-on	22
Standalone Web Workplace or AccessAssistant	23
Web Workplace from SSL VPN	23
Web Workplace Embedded in Enterprise Portal	24
Manage Application Credentials	24
Sign-up	24
Through AccessAssistant or Web Workplace	25
Through AccessAgent	25
Self-service	25
View Application Passwords	26

Reset Secrets 26

Reset Encentuate Password Using M of N Secrets 26

Modify User Profile 27

About this Guide

Conventions and Terminologies

The following conventions help the reader distinguish between different types of information:

Style	Description
<i>Italics</i>	Indicates navigation
Bold	Indicates dialog boxes, tabs, panels, fields, check box options, radio button options, field options, buttons, folder names and keys
<code>Courier New</code>	Indicates scripts, codes or commands
Green	Indicates cross-references
Blue	Indicates URLs

The acronyms used in this guide are listed below:

Acronym	Description
AD	Active Directory
HTML	Hypertext Markup Language
IMS	Encentuate IMS Server
J2EE	Java 2 Enterprise Edition
MAC	Mobile ActiveCode
OTP	One-Time Password
SSL	Secure Sockets Layer
UI	User Interface
URL	Uniform Resource Locator

Acronym	Description
VPN	Virtual Private Network
WAR	J2EE Web Archive

AccessAssistant and Web Workplace

With AccessAssistant and Web Workplace, enterprises can enjoy single sign-on without the hassle of deploying AccessAgent to client PCs, as long as enterprise applications are all Web-based. The Web automatic sign-on feature gives users the ability to log on to enterprise Web applications by simply clicking on links on AccessAssistant, Web Workplace, or enterprise portals, without the need to remember the passwords for individual applications. Users will just need to remember a single password to log on to all applications. Combined with the reverse proxy feature, Web automatic sign-on is able to support a very large variety of Web applications.

If AccessAgent is not deployed, users would have to sign up through other means. The enterprise can choose to integrate an identity provisioning system with IAM and provision users using it. Alternatively, users can sign up with IAM through AccessAssistant or Web Workplace. Just like signing up through AccessAgent, users would need to authenticate themselves by providing their enterprise directory password (for example, AD password) first, and then specify the Encentuate password and secret. Users can optionally choose to specify more secret questions and answers, which can be used by the self-service feature for password reset.

AccessAssistant and Web Workplace offer a host of self-service capabilities to the users. Users who usually use AccessAgent to log on to enterprise applications may need to know the application passwords when they use PCs that do not have AccessAgent installed. AccessAssistant allows users to view their application passwords or copy them to clipboard. Users can also reset their secret questions and answers through AccessAssistant or Web Workplace. Instead of having to call Helpdesk for an authorization code, the self-service feature allows users to reset their Encentuate passwords by providing a subset of the secrets that they have previously specified.

Users of AccessAgent will find the user interfaces of AccessAssistant and Web Workplace familiar because they have been designed to minimize the need for user training. For each user, the Wallet that can be accessed through AccessAgent, AccessAssistant, or Web Workplace is the same, and hence, the contents are fully synchronized across the user interfaces. System and user policies are all configured through AccessAdmin, making it easy for Administrators to configure all user interfaces from one central console.

AccessAssistant enables users to view application passwords, whereas Web Workplace does not. Its UI has been designed to facilitate the viewing of application passwords. On the other hand, Web Workplace's UI has been designed to look like a typical portal page, so as to facilitate logging on to enterprise Web applications. It can be integrated with customer's existing portal or SSL VPN, which AccessAssistant cannot.

This chapter covers the following topics:

- [Solution Overview](#)
- [General Prerequisites](#)
- [Installing AccessAssistant or Web Workplace](#)
- [Upgrading AccessAssistant and Web Workplace](#)
- [Embedding Web Workplace in Enterprise Portal](#)
- [Managing Policies](#)
- [Setting automatic web sign-on for AccessProfiles](#)
- [Workflow and Use Cases](#)

Solution Overview

This section specifies the high-level features of the product, as well as the deployment options for AccessAssistant and Web Workplace.

Product Specification

AccessAssistant and Web Workplace share a number of high-level requirements. These are described in the following sections.

Web Automatic Sign-on

Without installing any software (besides Web browser) on client PCs, users can enjoy automatic sign-on to Web application through AccessAssistant or Web Workplace. No change to Web applications is necessary, but not all types of Web applications are supported. Without reverse proxy (see next section), the following types of Web applications are not supported:

- Applications with logon pages using applets or complex JavaScript
- Applications with multiple-page logons
- Applications that require client-side certificate-based authentication
- Applications with logon pages involving Frames and iFrames
- Applications specifically designed to protect against automated/simulated logons
- Applications with logon pages that use Basic Authentication

The following Web browsers, in their default settings, are currently tested and supported. Since the product was not specifically designed for these Web browsers, it is possible that other Web browsers can be used too.

- Internet Explorer 5.0 and above on Windows
- Firefox 1.0 and above on Windows and Linux

Besides logging on to Web applications, users can also perform the following operations on the application credentials in their Wallets:

- Add/edit/delete application credentials

- Add more than one set of credentials for a single application
- For applications for multiple sets of credentials, select one to be the default account for automatic logon

Reverse Proxy

The reverse proxy feature enables AccessAssistant or Web Workplace to act as a Web proxy for users' access to certain enterprise Web applications. Users need not configure the Web proxy setting in the Web browser, but will need to access enterprise Web applications through URL links on AccessAssistant or Web Workplace. Since all accesses to those enterprise Web applications will need to pass through AccessAssistant or Web Workplace, the server hosting it will need to be sized appropriately. The advantage of this approach is that virtually all Web applications can now be supported since AccessAssistant or Web Workplace is acting as a Web client. The following types of Web applications are currently still not supported by reverse proxy, but it is possible to support them in the future:

- Applications with logon pages using applets or complex JavaScript
- Applications with multiple-page logons
- Applications that require client-side certificate-based authentication

Depending on the types of enterprise Web applications to be supported, customers can decide whether to use the reverse proxy feature for each enterprise Web application. Whether reverse proxy is used for an enterprise Web application is determined by the type of AccessProfile created for it.



The use of the term "reverse proxy" here does not imply that AccessAssistant and Web Workplace support most of the features that a typical reverse proxy server provides. It is only meant to widen the range of Web applications that AccessAssistant or Web Workplace can support.

User Sign-up

Since customers may not be deploying AccessAgent, users can choose to sign up through AccessAssistant or Web Workplace. Just like signing up through AccessAgent, users would need to authenticate themselves by providing their enterprise directory password (for example, AD password) first, and then specify the Encuentra password and secret. Users can optionally choose to specify more secret questions and answers, which can be used by the self-service feature for password reset.

Self-service

AccessAssistant and Web Workplace offer a host of self-service capabilities to the users. These are described in the sections below.

View Application Passwords

Users who usually use AccessAgent to log on to enterprise applications may need to know the application passwords when they use PCs that do not have AccessAgent installed. AccessAssistant allows users to view their application passwords or copy them to clipboard. Note that this feature is not available on Web Workplace.

Reset Secrets

Users can reset their secret questions and answers through AccessAssistant or Web Workplace. Note that users are currently not allowed to reset their primary (mandatory) secrets. All other secret questions and answers can be reset.

Reset Encentuate Password Using M of N Secrets

Instead of having to call Helpdesk for an authorization code, the self-service feature allows users to reset their Encentuate passwords by providing a subset (M) of the N secrets that they have previously specified. Both values M and N can be configured as policies on AccessAdmin. If the user cannot remember his secrets, he still has the option to reset his password by calling Helpdesk for an authorization code.

Modify User Profile

Users can modify the following user profile settings once they are logged on to AccessAssistant or Web Workplace:

- Mobile phone number for receiving Mobile ActiveCode (MAC)
- Email address for receiving MAC
- Preferred MAC delivery channel

Users can click either the **Save and test phone number** or **Save and test email address** button to request that the IMS Server send test messages to them when saving the settings. This feature allows users to keep the IMS Server updated with the latest user information.

Optional Two-factor Authentication

AccessAssistant and Web Workplace require users to authenticate themselves with at least the Encentuate password. If Encentuate password is configured to be synchronized with the AD password, users can also use their AD passwords to log on.

Administrators and Helpdesk can also configure user policies through AccessAdmin to enable two-factor authentication.

If two-factor authentication turned on for a user, he will need to supply one of the following, in addition to his Encentuate password, to log on:

- Authorization code issued by Helpdesk
- MAC, which can be sent to user via mobile phone or email.
- One-time Password (OTP) provided by an OTP token (for example, VASCO Digipass).

Synchronization of Wallets, AccessProfiles and Policies

AccessAssistant and Web Workplace are fully integrated with IMS Server to ensure that Wallets, AccessProfiles and policies are synchronized. This enables the following features:

- For each user, the Wallet that can be accessed through AccessAgent, AccessAssistant, or Web Workplace is the same, and hence, the contents are fully synchronized across the user interfaces.
- AccessAssistant and Web Workplace share the same AccessProfile framework with AccessAgent. Although it is not yet possible to use the same AccessProfile for both Web Workplace and AccessAgent, it will be possible in the near future to use AccessStudio to develop and manage AccessProfiles for Web Workplace. Currently, Web Workplace offers an AccessStudio-like Web interface for developing and managing its AccessProfiles.
- System and user policies for AccessAssistant and Web Workplace are all configured through AccessAdmin, making it easy for Administrators to configure all user interfaces from one central console.

Centralized Audit Logging

Actions that users perform in AccessAssistant and Web Workplace are centrally logged in the IMS Server. These audit logs, together with those reported by AccessAgent, can be viewed by Administrator or Helpdesk through AccessAdmin.

Integrated with SSL VPN

Aventail and Encentuate jointly provide a solution that delivers best-of-breed secure remote access from anywhere combined with two-factor authentication to ensure that only authorized users have access to corporate networks. With the solution, users can access Web, desktop, and legacy applications using an Aventail SSL VPN and ensure two-factor authentication through the use of a one-time Encentuate Mobile ActiveCode password delivered to smartphones, PDAs, pagers, fax, or other mobile devices.

Deployment Options

AccessAssistant and Web Workplace are packaged as WAR files that can be installed on any J2EE server, either on the same server as the IMS Server or on a

different server. Customer will have to decide whether to deploy AccessAssistant or Web Workplace, which have different features, as described in the following sections.

AccessAssistant

AccessAssistant has the following features:

- Web automatic sign-on
- Reverse proxy
- User sign-up
- View application passwords (All application credentials are listed. This includes applications that do not have AccessProfile for Web automatic sign-on.)
- Manage application credentials (All application credentials are listed. This includes applications that do not have AccessProfile for Web automatic sign-on.)
- Reset secrets
- Reset Encentuate password
- Modify user profile
- Optional two-factor authentication
- Synchronization of Wallets, AccessProfiles and policies
- Centralized audit logging

Since one of the main purposes of AccessAssistant is to assist users by retrieving application passwords, the UI has been designed to facilitate the viewing of application passwords.

Although AccessAssistant can also be configured to allow automatic sign-on to Web applications, it does not have the most efficient UI for that. If the primary objective is for users to perform automatic sign-on to Web applications, then Web Workplace should be deployed instead.

Web Workplace

Web Workplace has the following features:

- Web automatic sign-on
- Reverse proxy
- User sign-up
- Manage application credentials (Only applications that have AccessProfiles for Web automatic sign-on are listed.)
- Reset secrets
- Reset Encentuate password
- Modify user profile
- Optional two-factor authentication
- Synchronization of Wallets, AccessProfiles and policies
- Centralized audit logging
- Ability to be integrated with SSL VPN or enterprise portal

Since one of the main purposes of Web Workplace is to act as a portal for users to log on to enterprise Web applications, the UI has been designed to look like a typical portal page. Note that Web Workplace does not have the facility for users to view application passwords.

Web Workplace can be deployed in a few different ways, depending on whether it should be a standalone application or integrated with other systems like SSL VPN and enterprise portal. These deployment options are described in the following sections.

Standalone Web Workplace

Web Workplace can be deployed as a standalone application, which can act as an enterprise Web portal if the customer does not already have one.

Users log on directly to it by using Encentuate password with optional 2nd factor authentication (authorization code or MAC). Once logged on, users can perform automatic sign-on to enterprise applications by clicking on the application links in Web Workplace. If application credentials are not yet in the Wallet, Web Workplace will prompt user to supply the application credentials before attempting to perform automatic sign-on to the application.

Web Workplace on SSL VPN

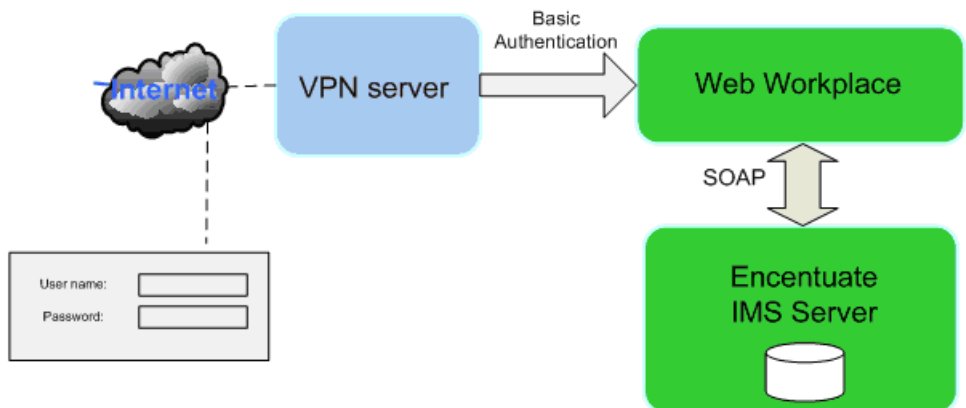
Web Workplace can be integrated with SSL VPN products. The following SSL VPN products have been tested and are supported by Web Workplace:

- Aventail
- Juniper

Web Workplace's URL should be configured as a Web shortcut on the SSL VPN's portal page. If supported by the SSL VPN, it should also be configured to perform single sign-on to Web Workplace using basic authentication. In this way, users can log on to the SSL VPN using the Encentuate password, which can, in turn, perform single sign-on to Web Workplace when users click the Web Workplace shortcut.

Alternatively, for better security, Web Workplace can be configured to authenticate users using both Encentuate password and MAC. In this case, users log on to the SSL VPN using Encentuate password, which, in turn, performs single sign-on to Web Workplace when users click on the Web Workplace shortcut. Users will then be prompted to provide either authorization code or MAC to log on to Web Workplace.

The SSL VPN can also be configured to authenticate users using both Encentuate password and MAC.



SSL VPN performing single sign-on to Web Workplace


















The table below summarizes the authentication options for Web Workplace on SSL VPN, with the assumption that the SSL VPN is using AD password for authentication:

Password Synchronization	SSL VPN Authentication	Web Workplace Authentication	Comments
Encentuate password not synchronized with AD password	AD password + (optional MAC)	Encentuate password + (optional MAC)	SSL VPN will not perform single sign-on to Web Workplace. Not recommended as user needs to authenticate twice.
Encentuate password synchronized with AD password	AD password	AD password (provided by SSL VPN)	SSL VPN performs single sign-on to Web Workplace.
Encentuate Password synchronized with AD password	AD password	AD password (provided by SSL VPN) + MAC (provided by user)	SSL VPN performs single sign-on to Web Workplace with AD password, but user has to supply MAC.
Encentuate Password synchronized with AD password	AD password + MAC	AD password (provided by SSL VPN)	Aventail SSL VPN and Juniper SSL VPN is able to perform single sign-on to Web Workplace, but other SSL VPNs may not.

Web Workplace Embedded in Enterprise Portal

If the customer already has an enterprise Web portal that users always visit, directly links for automatic sign-on to applications can be embedded in the portal. This means that a user can simply log on to the enterprise portal and click on application links, which will seamlessly bring him through Web Workplace. If he has not yet logged on to Web Workplace in that Web browser session, Web Workplace would prompt him for logon credentials. Subsequently, clicking on any application link in the enterprise portal would bring him straight to the application with sign-on automatically performed by Web Workplace.

The figure on the next page shows an example of embedding Web Workplace in an enterprise portal.

[Applications]	[Team Portals]
 Corporate Email  Corporate News  Apply for Leave  Apply for Course  Submit Claims  Service Request  Online Pay Slip  Annual Appraisal  Suggestion <hr/>  Yahoo! Mail  Hotmail  GMail  America Online  Income Tax Submission	 Administration  Finance  Engineering  Services  Sales <div style="background-color: #92d050; padding: 2px; text-align: center;">[Latest News]</div> <p>(Foster City, Calif., Feb. 22, 2006) – Encentuate, Inc., a provider of enterprise access security solutions, today announced that it has been declared a winner in the "Best Single Sign-On" and "Best Two-Factor Solution" categories by SC Magazine Awards 2006. In addition to the awards given, Encentuate was also nominated as a finalist in the "Best Authentication" category.</p>

Web Workplace embedded in an enterprise portal

Customers are recommended to also embed, in the enterprise portal, a link to Web Workplace so that users can perform the following functions by entering Web Workplace:

- Add multiple credentials for an application
- Change the default automatic logon credentials for an application, if it has multiple sets of credentials
- Edit/delete credentials for an application

Summary of AccessAssistant and Web Workplace Features

The following table is a summary of AccessAssistant and Web Workplace features. It serves as a reference for deciding between deploying AccessAssistant or Web Workplace.

High-level Features	AccessAssistant	Web Workplace
Web automatic sign-on	✓	✓
User sign-up	✓	✓
View application passwords	✓	
Manage application credentials	✓	✓
Reset secrets	✓	✓
Reset Encentuate password (knowledge-based or authorization code)	✓	✓
Modify user profile	✓	✓
Optional two-factor authentication	✓	✓

High-level Features	AccessAssistant	Web Workplace
Synchronization of Wallets, AccessProfile, and policies	✓	✓
Centralized audit logging	✓	✓
Ability to be integrated with SSL VPN or enterprise portal		✓

General Prerequisites

Use of Supported Web Browsers

Supported Web browsers should be used. The following Web browsers, in their default settings, are currently tested and supported:

- Internet Explorer 5.0 and above on Windows
- Firefox 1.0 and above on Windows and Linux

Since the product was not specifically designed for the above Web browsers, it is possible that other Web browsers can be used too. Customers or users should test any other Web browsers with AccessAssistant or Web Workplace before using them.

Cookies and JavaScript Enabled

Web automatic sign-on requires the following Web browser options to be enabled:

- Cookies
- JavaScript

As these are the default settings for the supported Web browsers, users should not need to perform any configuration on their Web browsers before starting to use AccessAssistant or Web Workplace.

Installing AccessAssistant or Web Workplace

To deploy AccessAssistant or Web Workplace in the same Tomcat instance that the IMS Server is running in:

- ❶ Stop IMS Server.
- ❷ Edit both **runserver.bat** in **\$IMS_INSTALL_FOLDER\$\ims\bin** folder and **installService.bat** in **\$IMS_INSTALL_FOLDER\$\ims\bin\installer** folder to include the system property: **accessAnywhere.configFile** that will specify the location of the accessAnywhere.properties file. For example: set **JAVA_OPTS=%JAVA_OPTS% DaccessAnywhere.config-File=%CATALINA_HOME%\accessAnywhere.properties**
- ❸ In a command prompt, go to the **\$IMS_INSTALL_FOLDER\$\ims\bin\installer** folder and run **installService changeit** where changeit is the keystore password.
- ❹ Copy the WAR file to **\$IMS_INSTALL_FOLDER\$**.
- ❺ Start IMS Server.

An AccessAssistant or WebWorkplace folder should be automatically created within **\$IMS_INSTALL_FOLDER\$**.

To deploy AccessAssistant or Web Workplace in another Web server:

- ❶ Stop the Web server that AccessAssistant or Web Workplace is going to be deployed in.
- ❷ Import the remote IMS Server's SSL certificate to the Web server's Java trust store.
- ❸ The trust store location is specified by the system property: **javax.net.ssl.trust-Store**
- ❹ The trust store password is specified by the system property: **javax.net.ssl.trust-StorePassword**
- ❺ The location of accessAnywhere.properties is specified by the system property: **accessAnywhere.configFile**
- ❻ **Modify server.xml** in conf folder. Under the tag **<Engine Name="StandAlone" defaultHost="localhost" debug="0">**, look for the "Host" tag and change the entries for **unpackWARS**, **autoDeploy** and **liveDeploy** to "true" as indicated:
<Host name="localhost" debug="0" appBase="/" unpackWARs="true" autoDeploy="true" liveDeploy="true">

- 7 Copy the WAR file to the webapps folder.
- 8 Start the Web server that is hosting the WAR file.
- 9 An AccessAssistant or WebWorkplace folder should be automatically created.

AccessAssistant and Web Workplace Configuration

Ensure that the `accessAnywhere.properties` file has been specified correctly as follows:

- **`accessAnywhere.properties`** file can be found in the **`config`** folder which is placed alongside the WAR file.
- The location of the **`accessAnywhere.properties`** file is specified by the system property **`accessAnywhere.configFile`**. If that is not found, the classpath is searched for the properties file.
- The **`config`** folder can be placed anywhere in the system as long as the system property `accessAnywhere.configFile` points to the path where **`accessAnywhere.properties`** can be found.

Edit the **`accessAnywhere.properties`** file and modify the keys below:

- `IMS_SERVER_HOSTNAME` should contain the hostname of the IMS Server.
- Modify any other keys as appropriate.
- Restart the IMS Server or hosting Web server for any configuration changes to take effect.

Upgrading AccessAssistant and Web Workplace

To upgrade AccessAssistant or Web Workplace:

- 1 Copy the **`accessAnywhere.properties`** file from the existing installation and save it somewhere for use later.
- 2 Delete the existing **AccessAssistant** or **WebWorkplace** folder.
- 3 Install the WAR file according to the instructions in [section 18](#).

- ④ Reinstall the **accessAnywhere.properties** file that was saved in the first step.
- ⑤ Restart the IMS Server or hosting Web server for the changes to take effect.

Embedding Web Workplace in Enterprise Portal

This feature allows users to click on a link in the enterprise portal to perform automatic sign-on to a Web application through Web Workplace. For each Web application to be embedded in the enterprise portal, use a URL of the form:

[https://WebWorkplace/
link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true](https://WebWorkplace/link_auto_logon.jsp?&acctClass=authserviceid&appName=appid&refresh=true)

where:

- WebWorkplace is the URL of Web Workplace.
- authserviceid is the authentication service ID to be used.
- appid is the application ID of the application.

The following is an example link: [https://preview.encentuate.com/WebWorkplace/
link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true](https://preview.encentuate.com/WebWorkplace/link_auto_logon.jsp?&acctClass=dir_yahoo&appName=app_yahoo_web&refresh=true)

Managing Policies

The following are the recommended policy settings for AccessAssistant and WebWorkplace:

User Policy Settings (Through AccessAdmin)

Policy ID	Value
Allow access to Wallet from AccessAssistant and Web Workplace?	True

Policy ID	Value
Second factor authentication required for AccessAssistant and Web Workplace?	(depends on customer preference)
Default second authentication factor for AccessAssistant and Web Workplace	(depends on customer preference)
Display personal authentication services in AccessAssistant and Web Workplace?	(depends on customer preference)

System Policy Settings (Through AccessAdmin)

Policy ID	Value
AccessAssistant and Web Workplace session timeout, in minutes	10
Duration for which passwords are displayed in AccessAssistant, in secs	60
Enable editing of user profile in AccessAssistant and Web Workplace?	True
Enable automatic sign-on to applications in AccessAssistant?	True
Password display option in AccessAssistant	2 (Display password by default, with option to copy to clipboard)
Enable self-service password reset?	True
Maximum number of secret questions a user should register to enable self-service	3
Number of secret questions a user needs to answer for using self-service.	2
The maximum number of invalid tries allowed before self-service locks out.	6
Reveal specific secret question ID when verification fails?	False

Setting automatic web sign-on for AccessProfiles

A user with Administrator role is able to author and manage Web AccessProfiles from AccessAssistant or Web Workplace. These additional options will be made available to Administrators:

- **Manage AccessProfiles:** To view, add, modify, or test Web AccessProfiles.
- **Synchronize system data with IMS Server:** To synchronize AccessProfiles and system policies with the IMS Server.

There are two types of Web AccessProfiles:

- **Dynamic AccessProfile:** This type of Web AccessProfile uses the reverse proxy feature. It can be used for virtually all kinds of Web applications. See [Reverse Proxy](#) section for details.
- **Static AccessProfile:** Web AccessProfiles that do not use the reverse proxy feature are static AccessProfiles. It typically uses a pre-stored logon form for logging on to the Web application.

The set of Web applications that can be supported by static AccessProfiles is a subset of those supported by dynamic AccessProfiles. However, we recommend the use of static AccessProfiles as far as possible because such AccessProfiles impose much less load on the AccessAssistant or Web Workplace server than dynamic ones.

Recommended procedures for creating a Web AccessProfile:

- ❶ Create a static AccessProfile for the application.
- ❷ Test the static AccessProfile.

OR

- ❶ Create a dynamic AccessProfile for it.
- ❷ Test the dynamic AccessProfile.

OR

- Modify the other AccessProfile parameters.

Using the Web AccessProfile Wizard

AccessAssistant and Web Workplace provide a wizard for creating Web AccessProfiles. The following sections describe the wizard workflow.

To create a new Web AccessProfile:

- ❶ Click **Manage AccessProfiles** in the left panel. At the bottom of the list of existing AccessProfiles, there is an **Add AccessProfile** button.
- ❷ Click the **Add AccessProfile** button to display the configuration page.

Step 1: Basic configuration

- ❶ **Logon page URL:** Enter the URL of the logon page. Be sure that the URL is not of a forwarding page.
- ❷ **Authentication service:** Select the authentication service from the drop-down list. If the desired authentication service cannot be found, click **Create new authentication service** to create a new authentication service.
- ❸ **Application:** Select the desired application to use from the drop-down list. If the desired application cannot be found, click **Create new application** to create a new application.
- ❹ **Account data template:** Select the appropriate description for the user name and password fields, where **ci** is “case-insensitive” and **cs** is “case-sensitive” (for example, “adt_ciuser_cspwd” means that the field requires a user name that is case-insensitive and a password that is case-sensitive).

Step 2: Download logon page

The Administrator should only continue with steps 2 through 6 if he wants to generate the recommended static AccessProfile. If a dynamic AccessProfile is desired, continue to step 7.

In this step, the Administrator should click the **Download logon page** button. This would fetch the page in a new browser window using the URL provided in step 1.

Step 3: Extract logon form

Click the **Extract logon form** button to extract the information from the logon form. This will be pre-stored and used for subsequent logon sessions.

Step 4: Load logon form

Click the **Load logon form** button to load the previously extracted logon form into the browser window, confirming that the logon form has been extracted accurately.

Step 5: Generate test signature

Click the **Generate test signature** button will generate a signature to be used for testing in step 6.

Step 6: Test

Click the **Proceed to test** button will use the generated test signature to test the logon form that was extracted.

If the test is successful and the Administrator sees that the test user name and password are injected into the logon fields of the form, click **Go to final step**.

If the test user name and password are not injected into the logon fields, the Administrator should either repeat the previous steps, or click the **Create dynamic AccessProfile** button. This would bring the Administrator to step 7.

Step 7: Download logon page

This step is used to generate a dynamic AccessProfile. This should be used only if the Administrator encounters problems with creating a static AccessProfile.

Click the **Download logon page** button to fetch the page in a new browser window using the URL provided in step 1.

Step 8: Generate test signature for dynamic AccessProfile

Click the **Generate test signature** button to generate a signature to be used for testing in step 9.

Step 9: Test

Click the **Proceed to test** button to use the generated test signature to test the logon page that was downloaded.

If the test is successful and the Administrator sees that the test user name and password are injected into the logon fields of the form, click **Go to final step**.

If the test user name and password are not injected into the logon fields, the Administrator should either repeat the previous steps or modify the script in step 8, then click **Go to final step**.

Final Step: Upload AccessProfile

In this final step, the Administrator will be able to modify any of the fields shown, if desired. If the settings generated by the wizard are satisfactory, click **Upload to IMS Server** to complete the AccessProfile generation process.

Workflow and Use Cases

AccessAssistant and Web Workplace support the following workflows and use cases:

- ❶ Web automatic sign-on
- ❷ Manage application credentials
- ❸ Sign-up
- ❹ View application passwords
- ❺ Reset secrets
- ❻ Reset Encuentra password

The use cases and workflows vary based on the deployment option:

- Whether AccessAssistant or Web Workplace has been deployed
- Whether Web Workplace is deployed standalone, with SSL VPN, or embedded in an enterprise portal

A user can access AccessAssistant or Web Workplace only if his user policy **Allow access to Wallet from AccessAssistant and Web Workplace?** is **True**.

Web Automatic Sign-on

Web Workplace can perform automatic sign-on to a Web application as long as an AccessProfile has been created for it. When user clicks on the Web application link, Web Workplace checks whether the user has any account for the authentication service tied to the Web application. If user has:

- **No account:** Web Workplace prompts user to enter a logon account. Subsequently user is automatically logged on to the application and the account is saved in user's Wallet.
- **One account:** User is automatically logged on using the account.
- **Multiple accounts, and a default one has been selected earlier:** User is automatically logged on using the default account.
- **Multiple accounts, and user has not selected a default:** Web Workplace asks user which account to use.

AccessAssistant can also perform automatic sign-on to Web applications if **Enable automatic sign-on to applications in AccessAssistant?** is **True**. All accounts are listed on the AccessAssistant UI. User clicks the **Log on** link of an account to log on to the corresponding application using the account credentials.

Standalone Web Workplace or AccessAssistant

The Web automatic sign-on workflow for a standalone Web Workplace or AccessAssistant is as follows:

- User goes to URL of AccessAssistant or Web Workplace.
- User is asked to enter Encentuate user name and password.
- User may need to enter an authorization code or MAC (depends on **Second factor authentication required for AccessAssistant and Web Workplace?** and **Default second authentication factor for AccessAssistant and Web Workplace**).
- User is brought to the AccessAssistant or Web Workplace home page.
- User is automatically logged on to a Web application when he clicks on the appropriate link.

Web Workplace from SSL VPN

The Web automatic sign-on workflow for accessing Web Workplace from SSL VPN is as follows. This workflow assumes that SSL VPN is using AD credentials and the Encentuate password is synchronized with the AD password, so that SSL VPN can use basic authentication to automatically log on to Web Workplace.

- User goes to URL for SSL VPN.
- User is asked to enter user name and password for SSL VPN.
- User enters Encentuate user name and password.
- SSL VPN authenticates the user with AD.
- After authentication, user sees the SSL VPN home page, where a link to Web Workplace is embedded.
- User clicks on the Web Workplace link.
- User is automatically brought to Web Workplace home page, if no additional authentication is required. If second factor authentication is required (**Second factor authentication required for AccessAssistant and Web Workplace?** is **True**), user is asked to enter the appropriate code (depends on **Default second authentication factor for AccessAssistant and Web Workplace**) before the Web Workplace home page appears.
- User clicks on any application link on Web Workplace to be automatically logged on to the application.

Web Workplace Embedded in Enterprise Portal

The Web automatic sign-on workflow for accessing Web applications through Web Workplace from an enterprise portal is as follows:

- User goes to URL for enterprise portal.
- User clicks on a link for an enterprise Web application.
- If user has not logged on to Web Workplace for the session, user is asked to enter Encentuate user name and password. If second factor authentication is required (**Second factor authentication required for AccessAssistant and Web Workplace? is True**), user is also asked to enter the appropriate code (depends on **Default second authentication factor for AccessAssistant and Web Workplace**).
- User is automatically signed-on to Web application.
- User can also click on Web Workplace link in the enterprise portal. User will be brought to the Web Workplace home page where he can modify user profile.

Manage Application Credentials

The workflow for editing application credentials is as follows:

- User has to access the Access Assistant or Web Workplace home page first.
- User clicks on appropriate link for editing application credentials.
- User may add new application credentials, or edit/delete existing application credentials.
- For Web Workplace, user may indicate the account to be used for automatic logon to the application. This will be the same account for automatic logon in AccessAgent. Conversely, if an account has been designated for automatic logon for an application in AccessAgent, it will also be used for automatic logon for the same application in Web Workplace.

Sign-up

Users may sign up through AccessAssistant or Web Workplace. This is especially useful for users who do not have access to AccessAgent.

Through AccessAssistant or Web Workplace

The workflow for signing up through AccessAssistant or Web Workplace is as follows:

- Users goes to the URL for AccessAssistant or Web Workplace.
- User clicks **Sign up** link.
- User enters user name and password for enterprise account (for example, AD credentials).
- User specifies Encentuate password.
- User chooses secret questions and provide the corresponding secret answers.

Through AccessAgent

If user signs up through AccessAgent, currently, he will only be able to specify his Encentuate password and mandatory secret question/answer. To specify the additional secret questions/answers, he will need to access Access Assistant or Web Workplace:

- User signs up through AccessAgent.
- User logs on to AccessAssistant or Web Workplace.
- User clicks **Reset my secrets** link.
- User chooses additional secret questions and provide the corresponding secret answers.

Self-service

AccessAssistant and Web Workplace offer the following self-service features to the users:

- View application passwords (only for AccessAssistant)
- Reset secrets
- Reset Encentuate password using M of N secrets
- Modify user profile

View Application Passwords

The workflow for viewing of application passwords is as follows. This feature is only available in AccessAssistant.

- User logs on to AccessAssistant.
- User clicks on appropriate link for the desired application account.
- Password can be viewed on the Web browser for a pre-defined amount of time (**Duration for which passwords are displayed in AccessAssistant, in secs**) or can be copied to clipboard (depends on **Password display option in AccessAssistant**).
- Depending on **Display personal authentication services in AccessAssistant and Web Workplace?**, passwords for personal applications can also be viewed.

Reset Secrets

The workflow for resetting of secrets is as follows:

- User logs on to AccessAssistant or Web Workplace.
- User clicks **Reset secrets** link.
- User may modify the existing optional secret questions and provide the corresponding secret answers. He will not get to see the existing secret answers.
- If user has not specified the optional secrets, he can also specify them through this page.
- Currently, user is not able to modify the mandatory secret question and answer.

Reset Encentuate Password Using M of N Secrets

User may reset Encentuate password using authorization code and secret through AccessAgent, AccessAssistant, or Web Workplace. AccessAssistant and Web Workplace also allow users to perform knowledge-based reset of Encentuate password (depends on **Enable self-service password reset?**) by using M (**Number of secret questions a user needs to answer for using self-service**) of their N (**Maximum number of secret questions a user should register to enable self-service.**) secrets. This workflow assumes that user has already specified at least M secrets:

- User goes to URL of AccessAssistant or Web Workplace.
- User clicks **Reset password**.

- User is asked to choose M questions and provide corresponding answers for them. Alternatively, he can reset password using authorization code.
- If any of the answers are wrong, user will be prompted to correct the answers (depends on **Reveal specific secret question ID when verification fails?**).
- If the maximum number of invalid trials (**The maximum number of invalid tries allowed before self-service locks out**) has been exceeded, the self-service capability will be locked for the user.

Modify User Profile

The workflow for modifying user profile is as follows:

- User logs on to AccessAssistant or Web Workplace.
- User clicks on **Change AccessAssistant settings** or **Change Web Workplace settings**.
- User may modify the mobile phone number or email for receiving MAC.
- User may also set the preferred MAC delivery channel.
- User may click either the **Save and test phone number** or **Save and test email address** button to request that the IMS Server send test messages to them when saving the settings.

